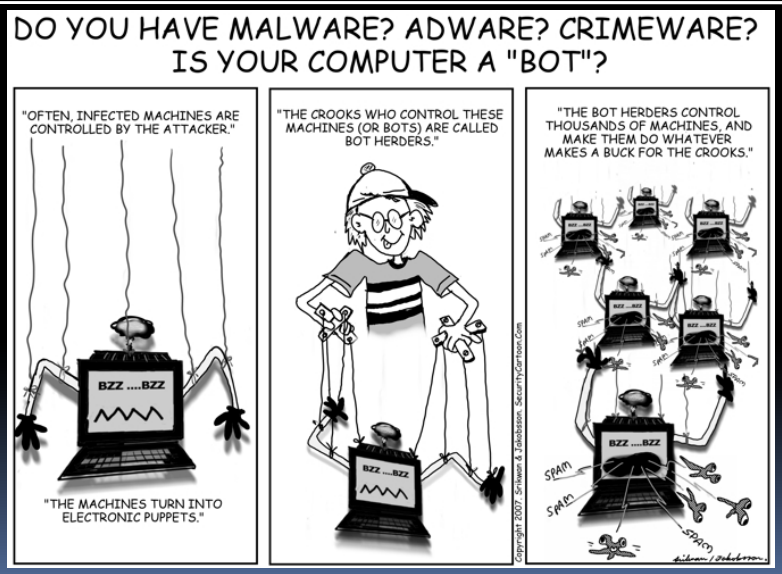
BOTNET-GENERATED SPAM

By Areej Al-Bataineh
University of Texas at San Antonio

MIT Spam Conference 2009

www.securitycartoon.com



Botnets: "A Global Pandemic"

Botnet is a network of compromised machines (Bots) under the command and control (C&C) of one person (master)

Machines become infected when users click on email attachments or URLs, visit malicious/legitimate web sites, or install software from untrusted sources

C&C protocols include IRC, HTTP, P2P

Botnets used for attacks like DDoS, spamming, phishing, identity theft, …etc

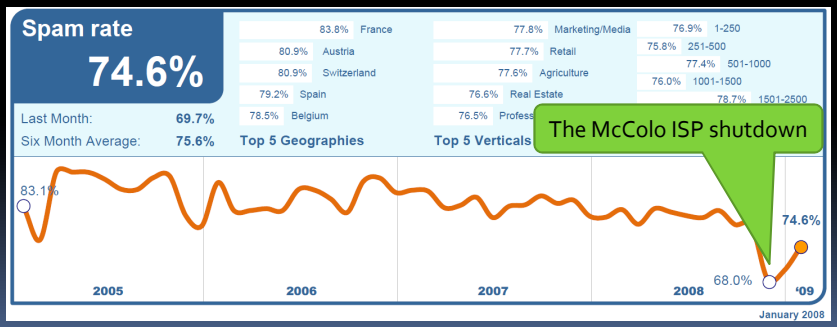
According Panda Labs, in 2Q 2008, 10 million bot computers were used to distribute spam and malware across the Internet each day

Botnets are mostly used for spamming!

According to Marshal's TRACE center :

In the 1Q of 2008, about 85% of spam is generated by 6 Botnets: Mega-D, Srizbi, Storm, Pushdo, Rustock, Cutwail.

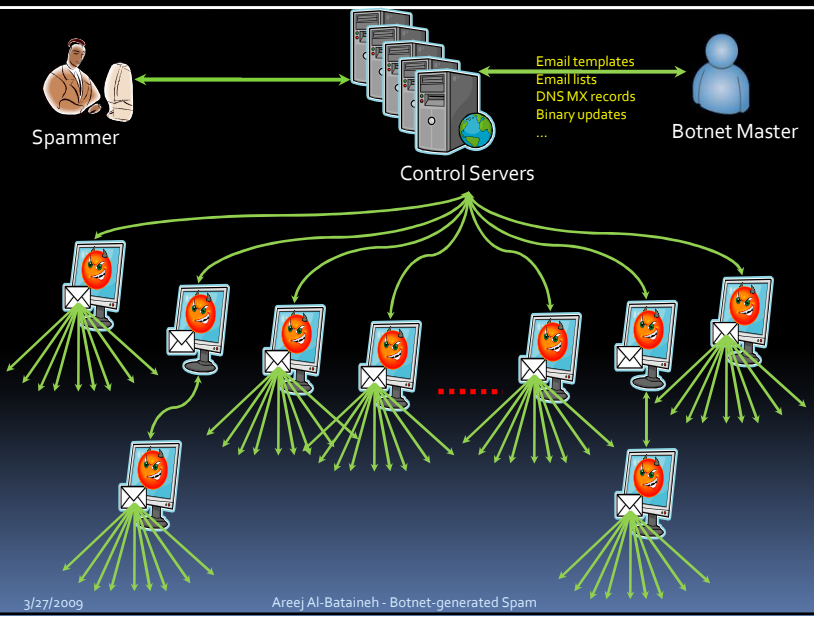
According to Symantec's Message Labs Intelligence:



Questions

- How does a typical spamming botnet work?
- How do botnets transmit spam?
- What can be done to make it nearly impossible for botnets to deliver spam?
- What tools and policies can be utilized at network edges?
- What tools and policies can be utilized at mail servers?

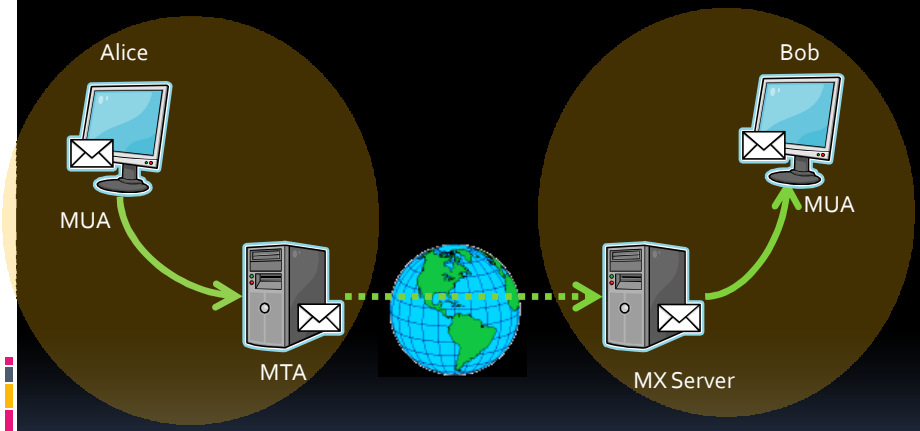
Spamming Botnet



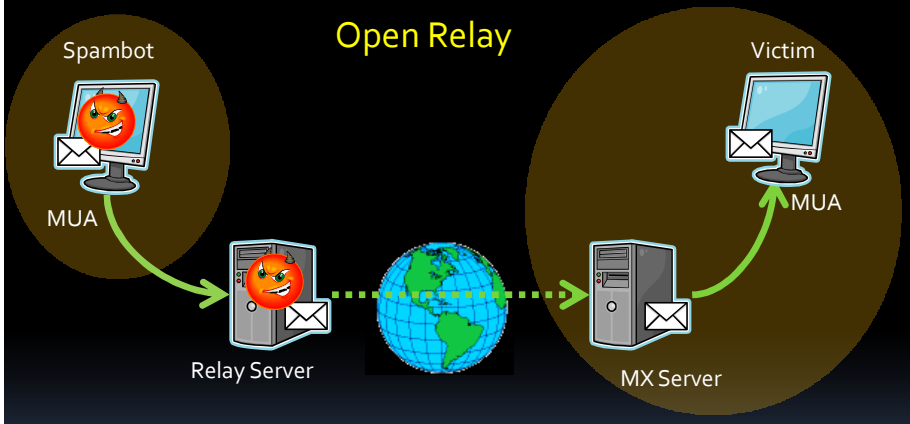
Questions

- How does a typical spamming botnet work?
- How do botnets transmit spam?
- What can be done to make it nearly impossible for botnets to deliver spam?
- What tools and policies can be utilized at network edges?
- What tools and policies can be utilized at mail servers?

Email Transmission



Spam Transmission 1

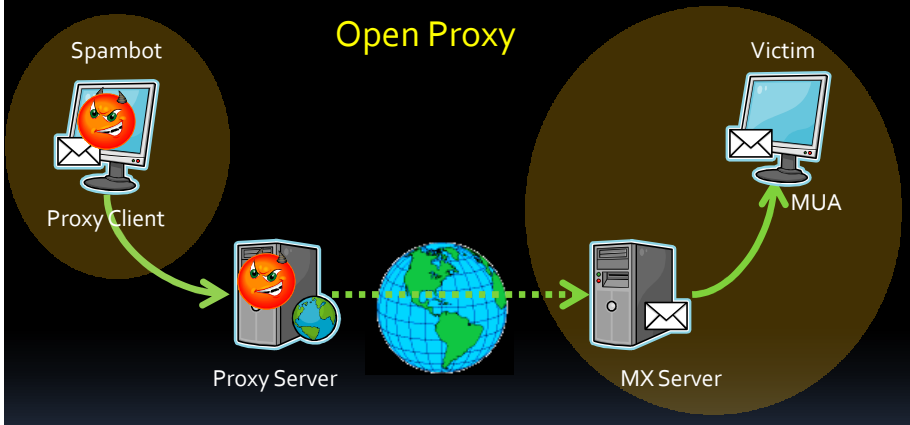


Spambot composes message according to the given template

Spambot forwards email to an open relay server

Mail server relays email to recipient mail server

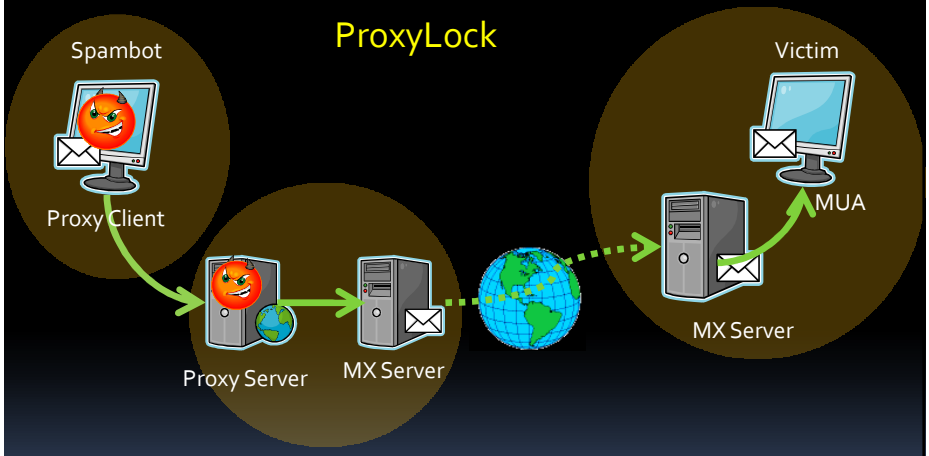
Spam Transmission 2



Spambot initiate a proxy connection (HTTP/SOCKS)

Proxy server forwards email traffic to a mail server

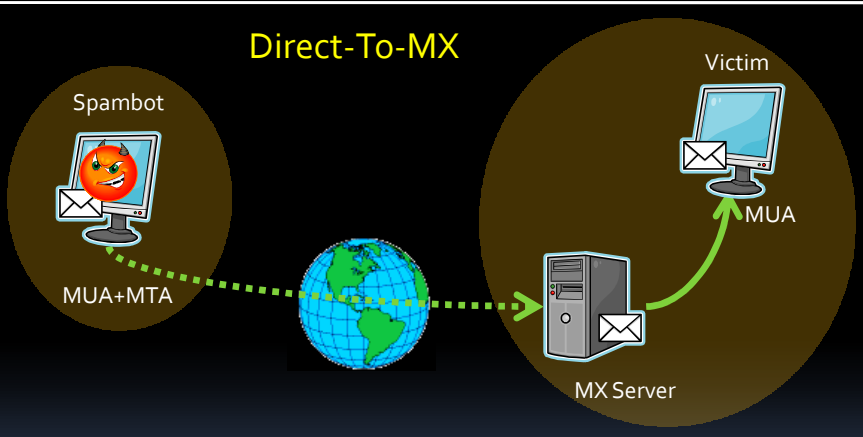
Spam Transmission 3



Spambot initiate a proxy connection (HTTP/SOCKS)

Proxy server forwards email traffic through mail server of its own domain

Spam Transmission 4

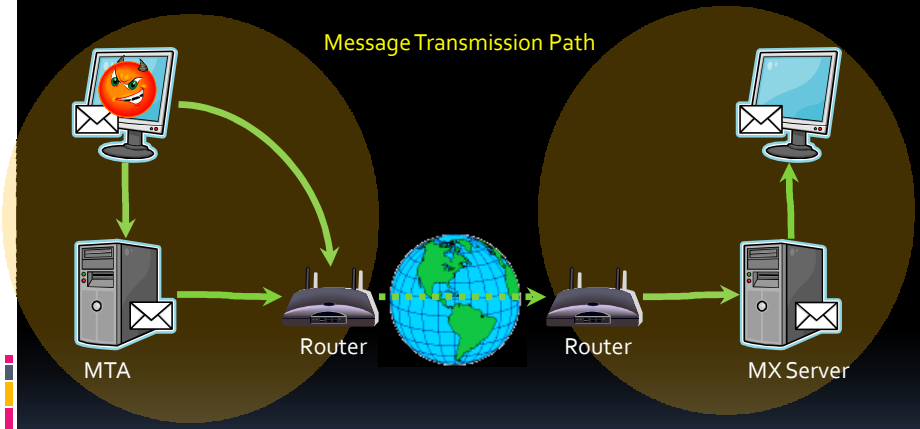


Spambot initiate SMTP connection with recipient mail server

Questions

- How does a typical spamming botnet work?
- How do botnets transmit spam?
- What can be done to make it nearly impossible for botnets to deliver spam?
- What tools and policies can be utilized at network edges?
- What tools and policies can be utilized at mail servers?

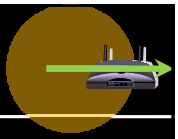
Spam Control



Questions

- How does a typical spamming botnet work?
- How do botnets transmit spam?
- What can be done to make it nearly impossible for botnets to deliver spam?
- What tools and policies can be utilized at network edges?
- What tools and policies can be utilized at mail servers?

Egress Spam control at Routers



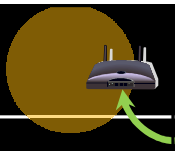
1. Manage port 25 traffic (*MAAWG 2008*)
   - Block mail traffic except from designated servers

   In some networks, this cannot be adopted!!
2. Monitor DNS queries (*Romana et al.* 2008)
   - Identify spambots within a network
   - based on their frequent DNS queries for MX records

   Some botnets maintains DB for MX records
3. DBSpam (*Xie et al.* 2006)
   - Block/throttle spam laundry traffic
   - Discover proxy bots inside the network

   Detect proxy traffic, not regular spam traffic

Ingress Spam Control at Routers



1. Local and dynamic Blacklists (*Cook et al. 2006*)
   - Identify IPs of spambots based on spam filters
   - Keep IPs in blacklists for a chosen period of time

   Spambots have dynamic IP addresses
2. Spam streams classification (*Argawal et al. 2005*)
   - Identify bulk email streams based on message similarities
   - Classify them as spam using a Bayesian classifier

   Template-based spam messages do not look similar
3. SpamFlow (Beverly & Sollins 2008)
   - Identify distinguishing features of spam TCP flows (RTT, idle, FIN)
   - Use machine learning classifier trained on open relay MTA mail connections

   Choosing the right features is key

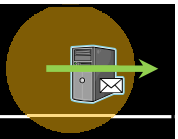
Summary – Control at Routers

Method	Direction	Effect
Cook	In	Block email traffic from locally-blacklisted sources
Argawal	In	Detect bulk spam traffic
SpamFlow	In	Detect spam TCP flows
Manage Port 25	Out	Drop email traffic except from legitimate outbound servers
Romana	Out	Detect spambots DNS MX queries
DBSpam	In/Out	Block/Throttle proxy traffic

Questions

- How does a typical spamming botnet work?
- How do botnets transmit spam?
- What can be done to make it nearly impossible for botnets to deliver spam?
- What tools and policies can be utilized at network edges?
- What tools and policies can be utilized at mail servers?

Spam Control at MTAs

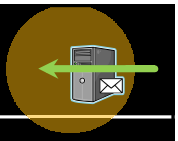


1. Email forwarding best practices
   - Specify inbound/outbound mail servers
   - Different port number (not 25) and user authentication

     spambot knows the port # and the user credentials
2. SMTP transaction Delay
   - Impose delay on suspicious requests
   - Suspicion based on SMTP RFCs compliance checks

     This delay will not affect spambots

Incoming Spam Control



1. Source IP address checking
   - Authorized mail server (SPF, DKIM, Sender ID)
     Spambots domain may not have such DNS records
   - Blacklists
     35% of spam comes from sources not listed in any blacklist
2. Greylisting
   - Refuse first delivery attempt, accept the second one
     Spambots can adapt and include this feature
3. SMTP session abort

Summary – Spam Control at Servers

Method	Direction	Effect
Reject open relays	In/Out	Block open relay attempts
Forwarding best practices	Out	Drop email from unauthorized users
SMTP delay	In	Delay spam and reduce its volume
Source IP checking	In	Drop email from untrusted servers
Greylisting	In	Refuse delivery attempts by untrusted sources
SMTP abort	In	Refuse delivery attempts from known suspicious sources

Review

Anti-spam is improving, but …

Why the spam volume is not decreasing?

Answer: Botnets

- Efficient Generation
- Guaranteed Delivery

Solutions: Spam control at …

- Routers or network edges
- Mail servers

Conclusions

- Botnet-generated spam:
  - Brings out new challenges
  - Opens new directions for solutions
- Intercepting spam while in transit is crucial
- New solutions should consider the nature of botnet-generated spam:
  - Distributed
  - Anonymous

Questions?

Comments?

Ideas?

hpp239@my.utsa.edu